ABSTRACT

Disclosed is an apparatus for encrypting/decrypting a real-time input stream. The present invention includes a control unit, a key schedule unit, and a block round unit. Accordingly, the present invention realizes the encryption and decryption of AES algorithm in a manner of hardware, thereby enabling to carry out the encryption and decryption of the real-time input stream real-timely. And, the present invention finds the key for encryption or decryption of one block every round when realizing the encryption and decryption of the AES algorithm in a hardware manner, and then outputs the found keys to the block round unit. The present invention reduces the size of the key register required for the encryption/decryption of block data, thereby enabling to reduce a size of hardware as well as cost of product.